# On reliability function of quantum communication channel

M. V. Burnashev [*], A. S. Holevo[†]

## 1. Introduction

Let $\mathcal{H}$ be a Hilbert space. We consider quantum channel [4] with a finite input alphabet $\{1, ..., a\}$ and with pure signal states $S_i = |\psi_i ><\psi_i|; i = 1, ..., a$. Compound channel of length $n$ is in the $n$–tensor product of the space $\mathcal{H}$, i.e. $\mathcal{H}_n = \mathcal{H} \otimes \ldots \otimes \mathcal{H}$. An input block (codeword) $u = (i_1, \ldots, i_n)$, $i_k \in \{1, \ldots a\}$, for it means using the compound state $\psi_u = \psi_{i_1} \otimes \ldots \otimes \psi_{i_n} \in \mathcal{H}_n$ and the corresponding density operator $S_u = |\psi_u ><\psi_u|$ in the space $\mathcal{H}_n$. A code $(\mathcal{C}, \mathbf{X})$ of cardinality $M$ in $\mathcal{H}_n$ is a collection of $M$ pairs $(u^1, X_1), \ldots, (u^M, X_M)$, where $\mathbf{X} = \{X_1, \ldots, X_M, X_{M+1}\}$ is a quantum decision rule, i.e. some resolution of identity in $\mathcal{H}_n$ [4]. The conditional probability $P(u^i|u^k)$ to make a decision in favor of message $u^i$ provided that message $u^k$ was transmitted is given by

$$P(u^i|u^k) = \mathrm{Tr}\, S_{u^k} X_i = <\psi_{u^k}|X_i\psi_{u^k}> \ .$$

In particular, the probability to make a wrong decision when the message $u^k$ is transmitted is

$$1 - \mathrm{Tr}\, S_{u^k} X_k = 1 - <\psi_{u^k}|X_k\psi_{u^k}> \ .$$

For given code $(\mathcal{C}, \mathbf{X})$ of cardinality $M$ we consider the following two error probabilities

$$\lambda_{max}(\mathcal{C}, \mathbf{X}) = \max_{1 \le k \le M}[1 - <\psi_{u^k}|X_k\psi_{u^k}>] \ ,$$

---

[*]Institute for Problems of Information Transmission, Russian Academy of Sciences.
[†]Steklov Mathematical Institute, Russian Academy of Sciences.

$$\bar{\lambda}(\mathcal{C}, \mathbf{X}) = \frac{1}{M} \sum_{k=1}^{M} [1 - < \psi_{u^k} | X_k \psi_{u^k} >] .$$

We shall denote by $P_e(M, n)$ any of the following two error probabilities

$$\lambda_{max}(M, n) = \inf_{\mathcal{C}, \mathbf{X}} \lambda_{max}(\mathcal{C}, \mathbf{X}), \qquad \bar{\lambda}(M, n) = \inf_{\mathcal{C}, \mathbf{X}} \bar{\lambda}(\mathcal{C}, \mathbf{X}).$$

It is well–known in classical information theory [1] (Corollary 2 to Theorem 5.6.2) that both $\lambda_{\max}(M, n)$ and $\bar{\lambda}(M, n)$ are essentially equivalent to each other. This remark obviously remains valid for quantum channels as well.

The Shannon capacity of quantum channel was naturally defined in [6] as the number $C$ such that $P_e(e^{nR}, n)$ tends to zero as $n \to \infty$ for any $0 \le R < C$ and does not tend to zero if $R > C$. Moreover, if $R < C$ then $P_e(e^{nR}, n)$ tends to zero exponentially with $n$ and we are interested in the logarithmic rate of convergence given by the reliability function

$$E(R) = \lim_{n \to \infty} \sup \frac{1}{n} \ln \frac{1}{P_e(e^{nR}, n)} , \quad 0 < R < C . \tag{1}$$

Our main results are the bounds for $E(R)$, reminiscent of the corresponding bounds in the classical information theory [1]. It is also remarkable that a number of tricks from the classical information theory works quite well for quantum channels.

Let $\pi = \{\pi_i\}$ be a probability distribution on the input alphabet $\{1, ..., a\}$, then we denote $\bar{S}_\pi = \sum_{i=1}^{a} \pi_i S_i$. Let $\lambda_j; j = 1, ..., d$, where $d$ is the dimension of $\mathcal{H}$, be the eigenvalues of operator $\bar{S}_\pi$ (obviously, forming a probability distribution). Then

$$H(\bar{S}_\pi) = -\mathrm{Tr}\bar{S}_\pi \ln \bar{S}_\pi = -\sum_{j=1}^{d} \lambda_j \ln \lambda_j \tag{2}$$

is the quantum entropy of the density operator $\bar{S}_\pi$. The upper bound for the capacity

$$C \le \max_\pi H(\bar{S}_\pi)$$

follows directly from the *entropy bound* [4]. Recently, in [2] the converse inequality $C \ge \max_\pi H(\bar{S}_\pi)$ was established, implying the formula

$$C = \max_\pi H(\bar{S}_\pi). \tag{3}$$

(This result was generalized to arbitrary signal states in [8]). The proof in [2] was based on the notion of typical subspace introduced in [9], [10]. A corollary of our estimates for the reliability function is an alternative approach to the converse inequality which makes no use of the notion of typical subspace.

## 2. The random coding lower bound

Let $\bar{\lambda}(u^1, \ldots, u^M)$ be the average error probability corresponding to codewords $u^1, \ldots, u^M$ of the input alphabet of the length $n$ minimized over all quantum decision rules. Let $\pi = \{\pi_i\}$ be a probability distribution on the input alphabet $\{1, \ldots, a\}$ and assume that the words are chosen at random, independently, and with the probability distribution

$$\mathsf{P}\{u = (i_1, \ldots, i_n)\} = \pi_{i_1} \cdot \ldots \cdot \pi_{i_n} \tag{4}$$

for each word.

**Proposition 1**. *For all $M, n$ and $0 \leq s \leq 1$*

$$\mathbf{E}\, \bar{\lambda}(u^1, \ldots, u^M) \leq 2(M-1)^s \left[ \mathrm{Tr}\, \bar{S}_\pi^{1+s} \right]^n , \tag{5}$$

*where*

$$\mathrm{Tr}\, \bar{S}_\pi^{1+s} = \sum_{j=1}^d \lambda_j^{1+s} .$$

*Proof.*[1] Let us for a while restrict to the subspace of $\mathcal{H}$ generated by the signal vectors $|\psi_i>; i = 1, \ldots, a$, and consider the Gram matrix $\Gamma(u^1, \ldots, u^M) = [<\psi_{u^i}|\psi_{u^j}>]$ and the Gram operator $G(u^1, \ldots, u^M) = \sum_{k=1}^M |\psi_{u^k}><\psi_{u^k}|$. This operator has the matrix $\Gamma(u^1, \ldots, u^M)$ in the (possibly overcomplete) basis

$$\hat{\psi}_{u^i} = G^{-1/2}(u^1, \ldots, u^M)\psi_{u^i} ; \quad i = 1, \ldots, M .$$

In [5] it was shown that using the resolution of identity of the form $X_k = |\hat{\psi}_k><\hat{\psi}_k|$ we can upperbound the average error probability as

$$\bar{\lambda}(u^1, \ldots, u^M) \leq \frac{2}{M} \mathrm{Sp}\left(E - \Gamma^{1/2}(u^1, \ldots, u^M)\right), \tag{6}$$

---

[1]The authors are grateful to T. Ogawa for pointing out an error in the earlier version of the proof.

3

where $E$ is the unit $M \times M$-matrix and Sp is the trace of $M \times M$-matrix. Indeed,

$$\bar{\lambda}(u^1, \ldots, u^M) = \frac{1}{M} \sum_{k=1}^{M} [1 - | < \psi_{u^k} | \hat{\psi}_{u^k} > |^2]$$

$$\leq \frac{2}{M} \sum_{k=1}^{M} [1 - | < \psi_{u^k} | \hat{\psi}_{u^k} > |] = \frac{2}{M} \sum_{k=1}^{M} [1 - < \hat{\psi}_{u^k} | G^{1/2}(u^1, \ldots, u^M) \hat{\psi}_{u^k} >],$$

which is (6).

The first step of our argument is to remark that

$$\frac{2}{M} \operatorname{Sp}(E - \Gamma^{1/2}(u^1, \ldots, u^M)) = \frac{2}{M}(M - \operatorname{Tr}G^{1/2}(u^1, \ldots, u^M)). \qquad (7)$$

In what follows we shall skip $u^1, \ldots, u^M$ from notations. Consider two operator inequalities

$$-2G^{1/2} \leq -2G + 2G,$$

$$-2G^{1/2} \leq -2G + (G^2 - G).$$

The first one is obvious, while the second follows from the inequality

$$-2x^{1/2} = 2(1 - x^{1/2}) - 2 = (1 - x^{1/2})^2 - 1 - x \leq (1 - x)^2 - 1 - x = x^2 - 3x,$$

valid for $x \geq 0$. Taking the expectation with respect to the probability distribution (3), we get

$$-2\,\mathbf{E}G^{1/2} \leq -2\mathbf{E}G + \begin{cases} 2\,\mathbf{E}G \\ \mathbf{E}(G^2 - G) \end{cases}.$$

Now

$$\mathbf{E}G = \mathbf{E} \sum_{k=1}^{M} |\psi_{u^k}>< \psi_{u^k}| = M\mathbf{E}|\psi_{u^k}>< \psi_{u^k}| = M\bar{S}_\pi^{\otimes n},$$

$$\mathbf{E}(G^2 - G) = \mathbf{E} \sum_{k=1}^{M}\sum_{l=1}^{M} |\psi_{u^k}>< \psi_{u^k}||\psi_{u^l}>< \psi_{u^l}| - \mathbf{E} \sum_{k=1}^{M} |\psi_{u^k}>< \psi_{u^k}|$$

$$= \mathbf{E} \sum_{k \neq l} |\psi_{u^k}>< \psi_{u^k}|\psi_{u^l}>< \psi_{u^l}| = M(M-1) \left[\bar{S}_\pi^{\otimes n}\right]^2.$$

Let $\{e_J\}$ be the orthonormal basis of eigenvectors, and $\lambda_J$ the corresponding eigenvalues of the operator $\bar{S}_\pi^{\otimes n}$. Then

$$-2\left\langle e_J|\mathbf{E}G^{1/2}|e_J\right\rangle \leq= -2M\lambda_J + M\lambda_J \min\left(2, (M-1)\lambda_J\right).$$

Using the inequality $\min\{a, b\} \leq a^s b^{1-s}$, $0 \leq s \leq 1$, we get

$$\min\left(2, (M-1)\lambda_J\right) \leq 2(M-1)^s \lambda_J^{1+s}, \ 0 \leq s \leq 1.$$

Summing with respect to $J$ and dividing by $M$, we get from (6), (7)

$$\mathbf{E}\,\bar{\lambda}(u^1, \ldots, u^M) \leq 2(M-1)^s \sum_J \lambda_J^{1+s} = 2(M-1)^s \left[\text{Tr}\,\bar{S}_\pi^{1+s}\right]^n, \ 0 \leq s \leq 1. \qquad \square$$

It is natural to introduce the function $\mu(\pi, s)$ similar to analogous function in classical information theory (e.g. [1], Ch. 5)

$$\mu(\pi, s) = -\ln \text{Tr}\,\bar{S}_\pi^{1+s} = -\ln \sum_{j=1}^d \lambda_j^{1+s}. \tag{8}$$

Clearly, $\mu(\pi, 0) = 0$. Using the formulas

$$\mu'(\pi, s) = -\frac{\text{Tr}\,\bar{S}_\pi^{1+s} \ln \bar{S}_\pi}{\text{Tr}\,\bar{S}_\pi^{1+s}},$$

$$\mu''(\pi, s) = \frac{(\text{Tr}\,\bar{S}_\pi^{1+s} \ln \bar{S}_\pi)^2 - \text{Tr}\,\bar{S}_\pi^{1+s}(\ln \bar{S}_\pi)^2 \text{Tr}\,\bar{S}_\pi^{1+s}}{(\text{Tr}\,\bar{S}_\pi^{1+s})^2},$$

it is easy to check that $\mu(\pi, s)$ is nondecreasing and $\cap$–convex function of $s$. Moreover,

$$\mu'(\pi, 0) = H(\bar{S}_\pi).$$

There is special case where among the signal vectors $|\psi_i\rangle; i = 1, \ldots, a$, there are $k \geq 1$ mutually orthogonal: then defining $\pi$ to be the uniform distribution on these vectors, one has $\mu(\pi, s) = s \ln k$. Otherwise the function $\mu(\pi, s)$ is strictly increasing and strictly $\cap$–convex (see Fig. 1).

By taking $M = e^{nR}$, we obtain

**Corollary 1.** *For any $0 < R < C$ the following lower bound holds*

$$E(R) \geq \max_\pi \max_{0 \leq s \leq 1} \left(\mu(\pi, s) - sR\right) \equiv E_r(R). \tag{9}$$

5

**Corollary 2.**

$$C \geq \max_{\pi} H(\bar{S}_{\pi}). \tag{10}$$

*Proof.* Indeed,

$$C \geq \max_{\pi} \max_{0 \leq s \leq 1} \frac{\mu(\pi, s)}{s} \geq \max_{\pi} \mu'(\pi, 0) = \max_{\pi} H(\bar{S}_{\pi}) \,.\; \Box.$$

Inequality (10) together with the converse inequality from [4] provides an alternative proof of the formula (3).

The maximization with respect to $s$ can be treated in the same way as in Ch. 5.7 of [1]. Defining the function

$$E_r(\pi, R) = \max_{0 \leq s \leq 1} [\mu(\pi, s) - sR], \tag{11}$$

we have

$$E_r(\pi, R) = \mu(\pi, 1) - R \quad \text{for} \quad 0 \leq R \leq \mu'(\pi, 1),$$

where

$$\mu(\pi, 1) = -\ln \mathrm{Tr} \bar{S}_{\pi}^2 = -\ln \sum_{i,j=1}^{a} \pi_i \pi_j | < \psi_i | \psi_j > |^2.$$

For $\mu'(\pi, 1) \leq R < C$ the function $E_r(\pi, R)$ is a $\cup$–convex and is given by

$$E_r(\pi, R) = \mu(\pi, s_R) - s_R R,$$

where $s_R$ is the root of the equation $\mu'(\pi, s_R) = R$ (see Fig. 2).

### 3. The expurgated lower bound

When we choose codewords randomly there is certain probability that some codewords will coincide that makes error probability for such code equal to 1. It turns out that probability to choose such a bad code does not influence essentially the average code error probability if the rate $R$ is relatively high. Conversely, it becomes dominating for low rates $R$. All these effects are well described in [1], Ch. 5.7. In order to reduce the influence of choosing such bad codes an elegant "expurgation" technique has been developed.

We start with an ensemble of codes with $M' = 2M - 1$ codewords and denote by

$$\lambda_k = [1 - | < \psi_{u^k} | \hat{\psi}_{u^k} > |^2]$$

the probability of erroneous decision for the word $u^k$, when the decision rule $\{X_k\}$ from Sec. 2 is used. Then according to the Lemma from Ch. 5.7 [1] there exists a code in the ensemble of codes with $M' = 2M - 1$ codewords, for which at least $M$ codewords satisfy

$$\lambda_k \leq [2\mathbf{E}\lambda_k^r]^{1/r} , \tag{12}$$

for arbitrary $0 < r \leq 1$ (without loss of generality we can assume that (12) holds for $k = 1, \ldots, M$). Then we can use an estimate from [2] to evaluate the righthand side of (12). By using the inequality $\sqrt{\gamma} \geq \frac{3}{2}\gamma - \frac{1}{2}\gamma^2$ for $\gamma \geq 0$, one obtains

$$\lambda_k \leq 2[1 - <\hat{\psi}_{u^k}|G^{\frac{1}{2}}(u^1, \ldots, u^{M'})\hat{\psi}_{u_k}>]$$

$$\leq 2 - 3 <\hat{\psi}_{u^k}|G(u^1, \ldots, u^{M'})\hat{\psi}_{u_k}> + <\hat{\psi}_{u^k}|G^2(u^1, \ldots, u^{M'})\hat{\psi}_{u_k}>$$

$$= \sum_{i \neq k} |<\psi_{u^i}|\psi_{u^k}>|^2,$$

where the summation is over $i$ from 1 to $M'$.

Using the inequality $(\sum a_i)^r \leq \sum a_i^r$, $0 < r \leq 1$, we get for randomly chosen codewords

$$\mathbf{E}\lambda_k^r \leq (M' - 1)\mathbf{E} |<\psi_u|\psi_{u'}>|^{2r} = 2(M - 1) \left[ \sum_{i,k=1}^{a} \pi_i \pi_k |<\psi_i|\psi_k>|^{2r} \right]^n .$$

Substituting this into (12) and denoting $s = \frac{1}{r}$, we obtain

**Proposition 2**. *For all* $s \geq 1$

$$\lambda_{max}(M, n) \leq \left( 4(M - 1) \left[ \sum_{i,k=1}^{a} \pi_i \pi_k |<\psi_i|\psi_k>|^{\frac{2}{s}} \right]^n \right)^s . \tag{13}$$

Taking $M = e^{nR}$, we obtain the lower bound with expurgation

$$E(R) \geq \max_{\pi} \max_{s \geq 1}(\tilde{\mu}(\pi, s) - s(R + \frac{\ln 4}{n})) \equiv E_{ex}(R + \frac{\ln 4}{n}),$$

where

$$\tilde{\mu}(\pi, s) = -s \ln \sum_{i,k=1}^{a} \pi_i \pi_k |<\psi_i|\psi_k>|^{\frac{2}{s}}.$$

7

The function $\tilde{\mu}(\pi, s)$ is $\cap$-convex, increasing from the value

$$\tilde{\mu}(\pi, 1) = \mu(\pi, 1) = -\ln \text{Tr} \bar{S}_\pi^2$$

for $s = 1$ to

$$\tilde{\mu}(\pi, \infty) = -\sum_{i,k=1}^{a} \pi_i \pi_k \ln |<\psi_i|\psi_k>|^2,$$

(which may be infinite if there are orthogonal states). The behavior of $\tilde{\mu}(\pi, s)$ in the case where this value is finite is shown on Fig. 1.

By introducing

$$E_{ex}(\pi, R) = \max_{s \geq 1}[\tilde{\mu}(\pi, s) - sR], \tag{14}$$

we can investigate the behavior of $E_{ex}(\pi, R)$ like in the classical case. Namely, for $0 < R \leq \tilde{\mu}'(\pi, 1)$, where

$$\tilde{\mu}'(\pi, 1) = -\ln \text{Tr} \bar{S}_\pi^2 + \frac{\sum_{i,k=1}^{a} \pi_i \pi_k |<\psi_i|\psi_k>|^2 \ln |<\psi_i|\psi_k>|^2}{\text{Tr} \bar{S}_\pi^2} \leq \tilde{\mu}(\pi, 1),$$

the function $E_{ex}(\pi, R)$ is $\cup$-convex decreasing from

$$E_{ex}(\pi, +0) = \tilde{\mu}(\pi, \infty) = -\sum_{i,k=1}^{a} \pi_i \pi_k \ln |<\psi_i|\psi_k>|^2 \tag{15}$$

to $E_{ex}(\tilde{\mu}'(\pi, 1)) = \tilde{\mu}(\pi, 1) - \tilde{\mu}'(\pi, 1)$. In the interval $\tilde{\mu}'(\pi, 1) \leq R \leq \tilde{\mu}(\pi, 1)$ it is linear function

$$E_{ex}(\pi, R) = \tilde{\mu}(\pi, 1) - R,$$

and $E_{ex}(\pi, R) = 0$ for $\tilde{\mu}(\pi, 1) \leq R < C$.

Thus comparing it with $E_r(\pi, R)$ we have in generic case the picture on Fig. 2:

$$\begin{aligned} E_r(\pi, R) &< E_{ex}(\pi, R), & 0 < R \leq \tilde{\mu}'(\pi, 1); \\ E_r(\pi, R) &= E_{ex}(\pi, R), & \tilde{\mu}'(\pi, 1) \leq R < \mu'(\pi, 1); \\ E_r(\pi, R) &> E_{ex}(\pi, R), & \mu'(\pi, 1) \leq R < C. \end{aligned}$$

However, it may happen that $\tilde{\mu}'(\pi, 1) > \mu'(\pi, 1)$, in which case the linear piece of the bound is absent.

The value (15) is in fact exact as the following proposition shows.

**Proposition 3.** *If $|<\psi_i|\psi_k>|>0$ for any $1\le i,k\le a$ then*

$$E(+0)=-\min_{\{\pi\}}\sum_{i,k=1}^{a}\pi_i\pi_k\ln|<\psi_i|\psi_k>|^2. \qquad (16)$$

*If $|<\psi_i|\psi_k>|=0$ for some $i,k$, then $E(+0)=\infty$.*

*Proof.* From (15) we see that $E(+0)$ is greater than or equal to the righthand side of (16). On the other hand, from testing two hypotheses ([3], p. 130, (2.34)), we have

$$\lambda_{max}(\mathcal{C},\mathbf{X})\ge\frac{1}{2}\left[1-\sqrt{1-\max_{u\ne u'}|<\psi_u|\psi_{u'}>|^2}\right]\ge\frac{1}{4}\max_{u\ne u'}|<\psi_u|\psi_{u'}>|^2,$$

where $u,u'$ are codewords from $\mathcal{C}=(u^1,\dots,u^M)$, and therefore

$$E(+0)\le-\lim_{n\to\infty}\left[\frac{2}{n}\max_{u\ne u'}\ln|<\psi_u|\psi_{u'}>|\right].$$

Denote $\psi_u(k)$ the $k$–th component of the codeblock $u$ and let $k_i=\pi_i M$ be the number of codeblocks $u$ with $\psi_u(k)=\psi_i$, $i=1,\dots,d$. Then we have

$$\max_{u\ne u'}\ln|<\psi_u|\psi_{u'}>|\ge\frac{1}{M(M-1)}\sum_{u,u'\in\mathcal{C}}\ln|<\psi_u|\psi_{u'}>|$$

$$\ge\frac{n}{M(M-1)}\min_{1\le k\le n}\sum_{u,u'\in\mathcal{C}}\ln|<\psi_u(k)|\psi_{u'}(k)>|$$

$$\ge\frac{n}{M(M-1)}\min_{\{k_i\}}\left\{\sum_{i=1}^{a}\sum_{j=1}^{a}k_ik_j\ln|<\psi_i|\psi_j>|\right\}$$

$$\ge\frac{nM}{(M-1)}\min_{\{\pi\}}\left\{\sum_{i=1}^{a}\sum_{j=1}^{a}\pi_i\pi_j\ln|<\psi_i|\psi_j>|\right\},$$

from where it follows

$$E(+0)\le-\min_{\{\pi\}}\sum_{i,k=1}^{a}\pi_i\pi_k\ln|<\psi_i|\psi_k>|^2.$$

In a result, we get (16).□

## 4. The binary quantum channel

Maximization of the bounds $E_r(\pi, R)$, $E_{ex}(\pi, R)$ over $\pi$, which is a difficult problem even in the classical case, is still more difficult in quantum case. However, if the distribution $\pi^0$ maximizing either $\mu(\pi, s)$ or $\tilde{\mu}(\pi, s)$ is the same for all $s$, then the analysis of Secs. 2, 3 applies to functions

$$E_r(R) = E_r(\pi^0, R), \qquad E_{ex}(R) = E_{ex}(\pi^0, R).$$

Let $a = d = 2$ and $|\psi_0>$, $|\psi_1>$ be two pure states with $|<\psi_0|\psi_1>| = \epsilon$. Consider the operator $S_\pi = (1 - \pi)S_0 + \pi S_1$. Its eigenvectors have the form $|\psi_0> + \alpha|\psi_1>$ with some $\alpha$. Therefore for its eigenvalues we get the equation

$$((1 - \pi)|\psi_0><\psi_0| + \pi|\psi_1><\psi_1|)\left(|\psi_0> + \alpha|\psi_1>\right) = \lambda\left(|\psi_0> + \alpha|\psi_1>\right).$$

Solving it, we find the eigenvalues

$$\lambda_1(\pi) = \frac{1}{2}\left[1 - \sqrt{1 - 4(1 - \epsilon^2)\pi(1 - \pi)}\right],$$

$$\lambda_2(\pi) = \frac{1}{2}\left[1 + \sqrt{1 - 4(1 - \epsilon^2)\pi(1 - \pi)}\right].$$

It is easy to check that both functions

$$\mu(\pi, s) = -\ln\left(\lambda_1(\pi)^{1+s} + \lambda_2(\pi)^{1+s}\right),$$

$$\tilde{\mu}(\pi, s) = -s\ln\left(\pi^2 + (1 - \pi)^2 + 2\pi(1 - \pi)\epsilon^{2/s}\right)$$

are maximized by $\pi = 1/2$. Denoting

$$\mu(s) = \mu(1/2, s) = -\ln\left[\left(\frac{1 - \epsilon}{2}\right)^{1+s} + \left(\frac{1 + \epsilon}{2}\right)^{1+s}\right],$$

$$\tilde{\mu}(s) = \tilde{\mu}(1/2, s) = -s\ln\left[\frac{1 + \epsilon^{2/s}}{2}\right],$$

we get the following bound

$$\begin{array}{ll}
E(R) \geq \tilde{\mu}(\tilde{s}_R) - \tilde{s}_R R, & 0 < R \leq \tilde{\mu}'(1); \\
E(R) \geq \mu(1) - R, & \tilde{\mu}'(1) \leq R \leq \mu'(1); \\
E(R) \geq \mu(s_R) - s_R R, & \mu'(1) \leq R < C,
\end{array}$$

where $\tilde{s}_R, s_R$ are solutions of the equations $\tilde{\mu}'(\tilde{s}_R) = R, \quad \mu'(s_R) = R,$

$$\mu(1) = \tilde{\mu}(1) = -\ln\left(\frac{1+\epsilon^2}{2}\right), \quad \tilde{\mu}'(1) = \tilde{\mu}(1) + \frac{\epsilon^2 \ln \epsilon^2}{1+\epsilon^2},$$

$$\mu'(1) = -\frac{(1-\epsilon)^2 \ln\left(\frac{1-\epsilon}{2}\right) + (1+\epsilon)^2 \ln\left(\frac{1+\epsilon}{2}\right)}{2(1+\epsilon^2)},$$

$$C = \mu'(0) = -\left[\left(\frac{1-\epsilon}{2}\right)\ln\left(\frac{1-\epsilon}{2}\right) + \left(\frac{1+\epsilon}{2}\right)\ln\left(\frac{1+\epsilon}{2}\right)\right].$$

Moreover, from Proposition 3,

$$E(+0) = -\ln \epsilon.$$

## 5. Comments on the case of arbitrary signal states

The case where the signal states are given by *commuting* density operators $S_i$ reduces to the case of classical channel with transition probabilities $\lambda_j^i$, where $\lambda_j^i$ are the eigenvalues of $S_i$. The classical bound given by Theorem 5.6.1 [1] in the case of commuting density operators takes the form

$$\mathbf{E}\bar{\lambda}(u^1, \ldots, u^M) \leq \min_{0 < s \leq 1} (M-1)^s \left(\mathrm{Tr}\left[\sum_{i=1}^a \pi_i S_i^{\frac{1}{1+s}}\right]^{1+s}\right)^n. \qquad (17)$$

The expurgated bound given by Theorem 5.7.1 of [1] in the case of commuting density operators reads

$$\lambda_{max}(M, n) \leq \min_{s \geq 1} \left(4(M-1)\left[\sum_{i,k=1}^a \pi_i \pi_k (\mathrm{Tr}\sqrt{S_i}\sqrt{S_k})^{\frac{1}{s}}\right]^n\right)^s. \qquad (18)$$

The righthand sides of (17), (18) are meaningful for arbitrary density operators, which gives some hope that these estimates could be generalized to the noncommutative case with minor modifications.

# References

[1] R. G. Gallager. Information theory and reliable communication. J. Wiley, NY 1968.

[2] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, W. Wooters, Classical information capacity of a quantum channel, Phys. Rev. A **54**, 1869-1876 (1996).

[3] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, NY, 1976.

[4] A. S. Holevo, Some estimates of the information transmitted by quantum communication channel, Probl. Peredachi Inform. **9**, 3-11 (1973) (rus); [Engl. Transl.: Probl. Inform. Transm. **9**, 177-183 (1973)].

[5] A. S. Holevo, On asymptotically optimal hypotheses testing in quantum statistics, Teor verojat. i ee primen., N 2, 429-432 (1978) (rus).

[6] A. S. Holevo, On the capacity of quantum communication channel, Probl. Peredachi Inform. **15**, 3-11 (1979) (rus); [Engl. Transl.: Probl. Inform. Transm. **15**, 247-253 (1979)].

[7] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory.* North Holland, Amsterdam, 1982.

[8] A. S. Holevo, The capacity of quantum channel with arbitrary signal states, LANL e-print quant-ph/9611023, 1996.

[9] B. Schumacher, Quantum coding, Phys. Rev. A **51**, N 4, 2738-2747 (1995).

[10] R. Jozsa, B. Schumacher, A new proof of the quantum noiseless coding theorem, J. Modern Optics, vol. 41, N 12, pp. 2343-2349 (1994).